

AUDIO TRANSCRIPTION OF RECORDING

Page 1	Page 3
<p>1</p> <p>2</p> <p>3</p> <p>4</p> <p>5 AUDIO RECORDING</p> <p>6 IN RE: STATE OF MISSOURI, ET AL.</p> <p>7 VS.</p> <p>8 JOSEPH R. BIDEN, JR., ET AL.</p> <p>9</p> <p>10 FILE: PREPARING FOR RETALIATORY ATTACKS FROM RUSSIA</p> <p>11 JUNE 29, 2022</p> <p>12</p> <p>13</p> <p>14 (Due to the quality of the recorded media, portions</p> <p>15 were unable to be transcribed and include inaudible</p> <p>16 portions. The transcript may also include</p> <p>17 misinterpreted words and/or unidentified speakers.</p> <p>18 The transcriber was not present at the time of the</p> <p>19 recording; therefore, this transcript should not be</p> <p>20 considered verbatim.)</p> <p>21</p> <p>22</p> <p>23</p> <p>24 TRANSCRIBED BY: MELISSA LANE</p> <p>25</p>	<p>1 ANNA DELANEY: So let's break that down,</p> <p>2 just specifically looking at the preparation.</p> <p>3 ELVIS CHANN: Yes.</p> <p>4 ANNA DELANEY: So where are the gaps first?</p> <p>5 ELVIS CHANN: So I think the gaps are that</p> <p>6 they haven't even mapped out their networks. They</p> <p>7 don't know where all of their most valuable data is.</p> <p>8 That's number one. And then number two is the</p> <p>9 backups. They typically will have online backups, but</p> <p>10 the problem is, with all the new variance of ransom</p> <p>11 ware, they look for the online backups, and they</p> <p>12 corrupt them. So the company's scratching their head,</p> <p>13 do I have offline backups, and if I do, have I ever</p> <p>14 restored from them? So that's like a second very</p> <p>15 large gap that we see. A third gap is their hair is</p> <p>16 on fire, and a lot of times they don't know who to</p> <p>17 call first. Am I going to call the CEO first? Am I</p> <p>18 going to call the CFO? Who am I going to call? When</p> <p>19 do I get external counsel involved? When do I get an</p> <p>20 incident response company involved? So those are the</p> <p>21 big three things that I see.</p> <p>22 ANNA DELANEY: What's blocking -- what's in</p> <p>23 the way companies in getting that all together?</p> <p>24 ELVIS CHANN: So I think -- I'm going to</p> <p>25 get a little existential right now. People don't</p>
Page 2	Page 4
<p>1 ANNA DELANEY: Hello. I'm Anna Delaney</p> <p>2 with ISMG, and I'm thrilled to be joined by Elvis</p> <p>3 Chann, cyber branch of the FBI San Francisco. Hi,</p> <p>4 Elvis.</p> <p>5 ELVIS CHANN: Hi, Anna. Thank you for</p> <p>6 having me.</p> <p>7 ANNA DELANEY: It's a great pleasure. So,</p> <p>8 Elvis, everybody's talking about ransom ware, and you</p> <p>9 speak -- see many, many portions, so where are the</p> <p>10 gaps in the ransom ware response plans?</p> <p>11 ELVIS CHANN: I definitely think -- well,</p> <p>12 number one, not having an incident response plan.</p> <p>13 ANNA DELANEY: Yeah.</p> <p>14 ELVIS CHANN: That's usually an issue, and</p> <p>15 then number two, I think the biggest gap is not having</p> <p>16 an established relationship with the FBI. So</p> <p>17 hopefully like step 13 or 15 on their incident</p> <p>18 response plan should be contacting law enforcement,</p> <p>19 and typically, for the companies that I don't have a</p> <p>20 relationship with, it's a Friday at 5:00 o'clock,</p> <p>21 before a long weekend, and they're frantic, and</p> <p>22 they've never dealt with us, and they don't know what</p> <p>23 we can bring to the table, and it's -- it's very</p> <p>24 Helter Skelter. I think those are the two biggest</p> <p>25 things that I see.</p>	<p>1 think they're ever going to be hacked, you know.</p> <p>2 Like, people -- you know, maybe I'm a little older</p> <p>3 now. I know I'm going to die at some point, but</p> <p>4 companies just don't think they're going to be hacked.</p> <p>5 So maybe they have some sort of incident response plan</p> <p>6 that's on a shelf collecting dust somewhere, but</p> <p>7 they've never done a table top exercise. They've</p> <p>8 never practiced it. They've never even looked at the</p> <p>9 incident response plan, because they never think</p> <p>10 they're going to get hacked. But guess what, ladies</p> <p>11 and gentlemen? I'm here to tell you, everyone is</p> <p>12 going to get hacked at some point, and you should be</p> <p>13 prepared for it.</p> <p>14 ANNA DELANEY: And part of that</p> <p>15 preparation, as you said earlier, is nurturing these</p> <p>16 relationships between law enforcement. What do you</p> <p>17 require for organizations? And I want to flip that</p> <p>18 around. What do you -- or how do you help or reach</p> <p>19 out to organizations as well?</p> <p>20 ELVIS CHANN: So -- so what do we require</p> <p>21 from organizations? So during an incident response</p> <p>22 plan, we will have questions; right? The most</p> <p>23 important things that we want to know when an incident</p> <p>24 has happened is, like, when did it happen? Do you</p> <p>25 have any logs that you can share with us, and then do</p>

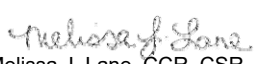
1 (Pages 1 to 4)

AUDIO TRANSCRIPTION OF RECORDING

Page 5	Page 7
<p>1 you have any evidence, do you have any attribution of</p> <p>2 who it could be, and then the last question is, do you</p> <p>3 know what data or, you know, money was stolen? So</p> <p>4 those are the things that we ask after an incident</p> <p>5 response.</p> <p>6 What we would like ahead of that is for the</p> <p>7 companies to already -- you can tell when a company's</p> <p>8 prepared. You can tell that when they've made the</p> <p>9 decision to call law enforcement, it's going to be</p> <p>10 their internal general counsel on the phone call.</p> <p>11 It's going to be their external attorney on the phone</p> <p>12 call, and they say, hey, Elvis, we want to talk to</p> <p>13 you. We've suffered from a security incident, and we</p> <p>14 would like to report this to you, and everything's</p> <p>15 lined up, everything's prepared. Like, we have logs,</p> <p>16 we're ready to share, how do you want us to get those</p> <p>17 to you? That's like a pie in the sky dream that</p> <p>18 rarely happens, to be honest with you, and that's</p> <p>19 fine; right? I want them to call us whenever it's</p> <p>20 happening, whenever they feel that they can get away</p> <p>21 from whatever they're doing.</p> <p>22 ANNA DELANEY: How do you reach out to</p> <p>23 organizations? How are you nurturing these relations?</p> <p>24 ELVIS CHANN: So we actually -- we have a</p> <p>25 rubric that we use with all the different things that</p>	<p>1 be number one. Number two is, have a good backup</p> <p>2 plan. Like, figure out what is your most important</p> <p>3 data and have backups of it. And specifically, also</p> <p>4 have offline backups; right? Cold storage and the</p> <p>5 reason for that, like I said before, ransom ware will</p> <p>6 look for your online backups and corrupt those as</p> <p>7 well. Number three is, you should have a telephone</p> <p>8 tree. I mean, a cell phone tree or what-have-you so</p> <p>9 that you have in prioritized order the phone calls</p> <p>10 that you will be making as a chief information</p> <p>11 security officer, who are the phone calls I need to</p> <p>12 make, and then number four is, oh, like, hopefully, if</p> <p>13 your e-mail went down or whatever your communication</p> <p>14 channel is, have backup communication channels; right?</p> <p>15 Whether it's an encrypted app or whether you spin up a</p> <p>16 Gmail account or something, you need to have backup</p> <p>17 communications, and then last but not least, I'm</p> <p>18 really hammering home on this, an incident response</p> <p>19 plan that you have practiced before.</p> <p>20 ANNA DELANEY: So midterm elections 2022.</p> <p>21 ELVIS CHANN: Yes.</p> <p>22 ANNA DELANEY: They're coming up.</p> <p>23 ELVIS CHANN: Yes, they are.</p> <p>24 ANNA DELANEY: What's the FBI doing to</p> <p>25 prepare?</p>
Page 6	Page 8
<p>1 you would think -- different metrics that -- that we</p> <p>2 really care about. Like, are they a Fortune 500</p> <p>3 company, are they some sort of strategic technology,</p> <p>4 are they one of the critical infrastructure sectors.</p> <p>5 And so what we do is, like, at the headquarters level,</p> <p>6 they rack and stack all of the different organizations</p> <p>7 in each field office's territory, and so for San</p> <p>8 Francisco, we -- it's called the systematically</p> <p>9 important partners program, and so we actually have</p> <p>10 over 278 companies that FBI headquarters is deemed</p> <p>11 that we need to have a relationship with these</p> <p>12 companies because they're strategically important to</p> <p>13 the national security of the United States, and I</p> <p>14 would say when they first rolled that out at the</p> <p>15 beginning of the year, we were already in an</p> <p>16 established relationship with 95 percent of those</p> <p>17 companies.</p> <p>18 ANNA DELANEY: What steps do you want to</p> <p>19 see organizations take to help you?</p> <p>20 ELVIS CHANN: So I -- I would like to just</p> <p>21 see the basics, to be honest with you. Like, the easy</p> <p>22 things are, let's do multifactor authentication. In</p> <p>23 my experience from the companies I work with here in</p> <p>24 the Silicon Valley, maybe only one out of every five</p> <p>25 companies does multifactor authentication. That would</p>	<p>1 ELVIS CHANN: So I think the good news is,</p> <p>2 post 2020, we've never stopped; right? Like, as soon</p> <p>3 as November 3rd happened in 2020, we just pretty much</p> <p>4 rolled into preparing for 2022. So at the FBI we are</p> <p>5 really engaged with our county registrars; right? So</p> <p>6 every field office is responsible for ensuring that</p> <p>7 they are in contact with each of the election</p> <p>8 officials in each of our countries; right? So that's</p> <p>9 where we deal -- we also meet regularly with the state</p> <p>10 level officials at the secretary of state.</p> <p>11 I think, you know, here in California, we</p> <p>12 just had our primary; right? On Tuesday. The good</p> <p>13 news is, it's all mail, so I mailed mine in a couple</p> <p>14 of weeks ago, but we also, I think, from FBI San</p> <p>15 Francisco's standpoint, we are also really engaged</p> <p>16 with the technology companies that are out here and</p> <p>17 represented here at the RSA conference, so making sure</p> <p>18 that, you know, any vulnerabilities we think advanced</p> <p>19 persistent threats would be using, specifically</p> <p>20 critical vulnerabilities that they get the message</p> <p>21 out, specifically to the election infrastructure</p> <p>22 organizations. We're also working with the social</p> <p>23 media companies to make sure that any foreign</p> <p>24 disinformation that's coming out that, you know, like</p> <p>25 if we can identify them, we can share that information</p>

2 (Pages 5 to 8)

AUDIO TRANSCRIPTION OF RECORDING

Page 9	Page 11
<p>1 with them so they can knock down accounts, knock down</p> <p>2 disinformation content, and then just having</p> <p>3 conversations with all of those organizations as</p> <p>4 they're building up to November of this year.</p> <p>5 ANNA DELANEY: What threats -- threat</p> <p>6 activity are you most concerned about?</p> <p>7 ELVIS CHANN: So I'm always the most</p> <p>8 concerned about advance persistent threats; right? So</p> <p>9 I think we saw in 2016, 2018, and to a lesser degree</p> <p>10 2020, the Russians. I guess the good or bad news is,</p> <p>11 they're kind of occupied right now with the Ukrainian</p> <p>12 invasion. What I've been telling companies that I'm</p> <p>13 very worried about and also sharing with critical</p> <p>14 infrastructure companies such as the election</p> <p>15 infrastructure is, at some point I'm very concerned</p> <p>16 that the Russians are going to launch cyber</p> <p>17 retaliatory attacks against the United States; right?</p> <p>18 Election infrastructure, transportation sector,</p> <p>19 financial sector, and energy sector are probably the</p> <p>20 four sectors that I'm the most worried about, and the</p> <p>21 FBI has been very actively engaged with the leaders in</p> <p>22 all of those sectors.</p> <p>23 ANNA DELANEY: Yeah. So rumor has it, we</p> <p>24 haven't seen anything massive yet; okay? But CISA</p> <p>25 warned this week or advised, please don't get too</p>	<p>1 insight.</p> <p>2 ELVIS CHANN: Thank you very much for</p> <p>3 having me, Anna.</p> <p>4 ANNA DELANEY: I've been speaking with</p> <p>5 Elvis Chann with the FBI, and for ISMG, I'm Anna</p> <p>6 Delaney.</p> <p>7 (Audio ended.)</p> <p>8</p> <p>9</p> <p>10</p> <p>11</p> <p>12</p> <p>13</p> <p>14</p> <p>15</p> <p>16</p> <p>17</p> <p>18</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24</p> <p>25</p>
Page 10	Page 12
<p>1 complacent. So what should organizations be doing to</p> <p>2 prepare for, as you say, a potential retaliation here?</p> <p>3 ELVIS CHANN: Yeah. So definitely I</p> <p>4 completely agree with CISA on this. There's three</p> <p>5 types of attacks that I'm thinking are going to</p> <p>6 happen. Number one are going to be coordinated ransom</p> <p>7 ware attacks because we know the preponderance of</p> <p>8 ransom ware actors are actually in Russia. That's</p> <p>9 number one. Number two are data wiping attacks, so</p> <p>10 we've seen a lot of that going on in Ukraine right</p> <p>11 now. You know, we work very closely with the</p> <p>12 Ukrainian government, and that is definitely something</p> <p>13 that they've seen. Number three is continued spear</p> <p>14 fishing campaigns, trying to steal credentials, trying</p> <p>15 to elicit information from people in all of the</p> <p>16 sectors that I mentioned. Those are the three types</p> <p>17 of attacks. So I would say, come back to, how do we</p> <p>18 protect against those three types of attacks? It's</p> <p>19 the basic cyber security things, having multifactor</p> <p>20 authentication, having, you know, patch networks,</p> <p>21 having good firewalls and -- and all of the basic</p> <p>22 stuff will prevent maybe 80 to 90 percent of those</p> <p>23 attacks that I just mentioned.</p> <p>24 ANNA DELANEY: Elvis, this has been such a</p> <p>25 pleasure. Thank you very much for sharing your</p>	<p>1 CERTIFICATE OF REPORTER</p> <p>2</p> <p>3 I, Melissa J. Lane, Certified Court</p> <p>4 Reporter of Missouri, Certified Shorthand Reporter of</p> <p>5 Illinois and Registered Professional Reporter, do</p> <p>6 hereby certify that I was asked to prepare a</p> <p>7 transcript of proceedings had in the above-mentioned</p> <p>8 case, which proceedings were held with no court</p> <p>9 reporter present utilizing an open microphone system</p> <p>10 of preserving the record.</p> <p>11 I further certify that the foregoing pages</p> <p>12 constitute a true and accurate reproduction of the</p> <p>13 proceedings as transcribed by me to the best of my</p> <p>14 ability and may include inaudible sections or</p> <p>15 misidentified speakers of said open microphone</p> <p>16 recording.</p> <p>17</p> <p>18  Melissa J. Lane, CCR, CSR, RPR</p> <p>19</p> <p>20</p> <p>21</p> <p>22</p> <p>23</p> <p>24 Date:</p> <p>25</p>

3 (Pages 9 to 12)